PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 4414-38	**FOR FURTHER ACTION**	see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.
International application No. PCT/US04/21846	International filing date (*day/month/year*) 09 July 2004 (09.07.2004)	(Earliest) Priority Date (*day/month/year*) 10 July 2003 (10.07.2003)
Applicant RSA SECURITY INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 4 sheets.

☒ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the Report**
   a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.
   ☐ the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).
   b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing:
   ☐ contained in the international application in written form.
   ☐ filed together with the international application in computer readable form.
   ☐ furnished subsequently to this Authority in written form.
   ☐ furnished subsequently to this Authority in computer readable form.
   ☐ the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
   ☐ the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.
2. ☐ **Certain claims were found unsearchable** (See Box I).
3. ☐ **Unity of invention is lacking** (See Box II).
4. With regard to the **title**,
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,
   ☐ the text is approved as submitted by the applicant.
   ☒ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No. 2
   ☒ as suggested by the applicant. ☐ None of the figures
   ☐ because the applicant failed to suggest a figure.
   ☐ because this figure better characterizes the invention.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US04/21846

Box III TEXT OF THE ABSTRACT (Continuation of Item 5 of the first sheet)

The technical features mentioned in the abstract do not include a reference sign between parentheses (PCT Rule 8.1(d)).

NEW ABSTRACT

Techniques for secure generation of a seed for use in performing one or more cryptographic operations, utilizing a seed generation protocol carried out by a seed generation client [110c] and a seed generation server [110s]. The seed generation server [110s] provides a first string to the seed generation client [110c]. The seed generation client [110c] generates a second string, encrypts the second string utilizing a key [216], and sends the encrypted second string to the seed generation server [110s]. The seed generation client [110c] generates the seed as a function of at least the first string and the second string. The seed generation server [110s] decrypts the encrypted second string [222] and independently generates the seed as a function of at least the first string and the second string.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/21846

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : H04L 9/00
US CL : 380/46
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 380/46

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6,189,098 B1 (KALISKI, JR.) 13 February 2001 (13.02.2001), column 2, lines 27-53.	1-40
A	US 5,963,646 (FIELDER et al.) 05 October 1999 (05.10.1999), column 3, lines 18-55.	1-40
X	US 6,125,186 (SAITO et al.) 26 September 2000 (26.09.2000), column 1, line 45 to column 2, line 5, column 4, lines 3-65.	1-40
A	US 6,148,404 (YATSUKAWA) 14 November 2000 (14.11.2000), column 11, line 2 to column 13, line 67.	1-40

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
04 November 2004 (04.11.2004)	24 NOV 2004
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703) 305-3230	Authorized officer Ayaz Sheikh Telephone No. (703)305-3900

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

PCT/US04/21846

Continuation of B. FIELDS SEARCHED Item 3:
EAST, IEEE, ACM
search terms: seed generating, key exchange, generating keys

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/21846

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : H04L 9/00
US CL : 380/46
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 380/46

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6,189,098 B1 (KALISKI, JR.) 13 February 2001 (13.02.2001), column 2, lines 27-53.	1-40
A	US 5,963,646 (FIELDER et al.) 05 October 1999 (05.10.1999), column 3, lines 18-55.	1-40
X	US 6,125,186 (SAITO et al.) 26 September 2000 (26.09.2000), column 1, line 45 to column 2, line 5, column 4, lines 3-65.	1-40
A	US 6,148,404 (YATSUKAWA) 14 November 2000 (14.11.2000), column 11, line 2 to column 13, line 67.	1-40

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
04 November 2004 (04.11.2004)

Date of mailing of the international search report
24 NOV 2004

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (703) 305-3230

Authorized officer
Ayaz Sheikh Peggy Harrod
Telephone No. (703)305-3900

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

PCT/US04/21846

Continuation of B. FIELDS SEARCHED Item 3:
EAST, IEEE, ACM
search terms: seed generating, key exchange, generating keys